THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, Plaintiff, v. MICROSOFT CORPORATION, Defendant.	CASE NO. C11-1438-JCC ORDER

This matter comes before the Court on Defendant's motion for summary judgment (Dkt. No. 100) and Plaintiff's motion for class certification (Dkt. No. 70). Having thoroughly considered the parties' briefing and the relevant record, the Court finds oral argument unnecessary and hereby GRANTS the summary-judgment motion and DISMISSES as moot the class-certification motion for the reasons explained herein.

I. BACKGROUND

This case concerns Microsoft's Windows Mobile 7 operating system—in particular, when and how the phone's software accessed stored location information.

A. Location Framework Platform

The "location framework" was a software component of the Windows Mobile 7 operating system. (Dkt. No. 100 at 9; Dkt. No. 105 at 7.) Software applications, such as search or mapping services, "called" this framework in order to obtain location information to incorporate into the applications' services. (Dkt. No. 100 at 9; Dkt. No. 105 at 7.) When the location framework received a call from an application, it could resolve the location request in one of several ways. (Dkt. No. 100 at 10; Dkt. No. 105 at 8.) Most relevant in this case were the ways that the location framework resolved requests using "beacons."[1] (Dkt. No. 100 at 10; Dkt. No. 105 at 8–9.)

Beacons are sources of signals in the world, such as Wi-Fi access points or cell towers. (Dkt. No. 100 at 10; Dkt. No. 105 at 7.) Each beacon transmits unique identifying data and can be identified accordingly. (Dkt. No. 105 at 7.) This has allowed Microsoft to compile a database called "Orion," which contains location information about the latitude and longitude of beacons around the world. (Dkt. No. 91 ¶ 9; Dkt. No. 100 at 10; Dkt. No. 105 at 7.) A Windows Phone 7 device interacted with Orion and could both send and receive information about the locations of beacons. (Dkt. No. 91 ¶¶ 9, 16; Dkt. No. 105 at 9.) Orion transmitted beacon data to a phone in the form of "tiled" data or "tiles." (Dkt. No. 91 ¶9; Dkt. No. 105 at 8.) "The tiles are best visualized as rectangular excerpts from Orion's larger map of beacons in the area." (Dkt. No. 91 ¶ 9.) Tiles were stored in the phone's random access memory ("RAM"),[2] and stayed on the phone for roughly ten days before being discarded as stale. (Dkt. No. 91 ¶14.)

Upon receiving a location request, the location framework looked for nearby visible beacon signals. (Dkt. No. 100 at 10; Dkt. No. 105 at 8.) The location framework then looked at the information about beacons contained on the RAM-stored tiles. (Dkt. No. 100 at 11; Dkt. No. 105 at 8–9.) If the two sets of beacon data matched—i.e., if the tiles contained location information for the "seen" beacons—then the location framework could ascertain the phone's location, and the framework returned that location to the requesting application. (Dkt. No. 100 at

[1] The location framework could also resolve location requests by using global positioning signals (GPS). (Dkt. No. 100 at 10; Dkt. No. 105 at 9.) Obtaining location data by GPS took longer and used more processing power than obtaining location data by using beacon positioning. (Dkt. No. 70 at 3.)

[2] Tiles were also stored in flash memory (Dkt. No. 105 at 8–9), but that additional storage location does not affect the legal analysis.

11; Dkt. No. 105 at 8–9.) If the “seen” beacons did not match the tiles, then the location framework called Orion for new tile data. (Dkt. No. 100 at 11; Dkt. No. 105 at 5.) If the new tiles contained relevant data, then the location framework returned a location to the requesting application. (Dkt. No. 105 at 5.) As this description suggests, some location requests were resolved entirely on the phone, so not every location request necessarily involved transmitting data to or from Orion. (Dkt. No. 69 at 12; Dkt. No. 100 at 11.)

B. Permission to use location

Generally, users had to consent to allowing applications to make calls to the location framework. (Dkt. No. 100 at 9–10; Dkt. No. 105 at 7–8.) Each phone had a master switch for location services in its settings menu. (Dkt. No. 91 ¶ 4.) With one exception not relevant here,[3] applications could access the location framework only if this setting was turned “on.” (Dkt. No. 91 ¶ 4.)

In addition to the master location switch, the individual camera application asked the user a question about location services. When a user first ran the camera application, the phone displayed the following user prompt:

> **Allow the camera to use your location?**
>
> Sharing this information will add a location tag to your pictures so you can see where your pictures were taken. This information also helps us provide you with improved location services. We won’t use the information to identify or contact you.

(Dkt. No. 105 at 10.) The user could either press “allow” or “cancel.” (*Id.*) If the user closed the dialog box without choosing one of these options, the box would continue to open every time the camera application was opened until the user made a choice. (Dkt. No. 105 at 6 n.5.)

Importantly for this case, even if the user hit “cancel” the camera application called the

[3] The Find My Phone application can always access location services. (Dkt. No. 100 at 10.)

location framework each time the application was opened, and the framework then always accessed the phone's RAM data. (Dkt. No. 105 at 10.)

C. Plaintiff's use of the camera application

Plaintiff Rebecca Cousineau began using a smartphone that ran the Windows 7 operating system in June 2011. (Dkt. No. 105 at 10.) Ms. Cousineau used the phone's location services on some occasions, such as to obtain driving directions from the phone's map application. (Dkt. No. 105 at 10.) Ms. Cousineau did not, however, press "allow" at the camera application's user prompt concerning location services. (Dkt. No. 105 at 11.)

II. DISCUSSION

D. Standard on Summary Judgment

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Material facts are those that may affect the case's outcome. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A dispute about a material fact is genuine if there is enough evidence for a reasonable jury to return a verdict for the nonmoving party. *See id.* at 49. At the summary judgment stage, evidence must be viewed in the light most favorable to the nonmoving party, and all justifiable inferences must be drawn in the nonmovant's favor. *See Johnson v. Poway Unified Sch. Dist.*, 658 F.3d 954, 960 (9th Cir. 2011).

E. The Stored Communications Act

Plaintiff alleges that the manner in which her location data was accessed constitutes unlawful access to a stored communication in violation of the Stored Communications Act ("SCA"). (Dkt. No. 69 at 2.) The Ninth Circuit has described the background of the SCA:

> The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, [citation omitted], the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

The particular provision at issue in this case is a "close cousin" to a provision in the Computer Fraud and Abuse Act (CFAA). Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1239 (2004). "Federal courts interpreting [the SCA and the CFAA] have noted that their 'general purpose . . . was to create a cause of action against 'computer hackers (e.g., electronic trespassers).'" *International Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005) (citing cases). Under the provision at issue in this case, it is an offense to:

> (1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceed[] an authorization to access that facility;
>
> and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system."

18 U.S.C. § 2701(a).

This case implicates 18 U.S.C. § 2701(a)(2), which involves "exceed[ing] authorized access." (Dkt. No. 105 at 24; Dkt. No. 109 at 9.) In interpreting this phrase, courts have described "exceeding authorized access" as occurring when a party accesses information that the party has no authority to see, or information that is stored in a place where the party has no authority to be. *See International Ass'n of Machinists*, 390 F.Supp.2d at 496–97 (no violation of SCA when individual was "entitled to see" the information); *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, 821 (E.D. Mich. 2000) ("Section 2701 outlaws illegal entry, not larceny."). As one court wrote, "the sort of trespasses to which the Stored Communications Act applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way." *Educational Testing Serv. v. Stanley H. Kaplan Educ. Ctr.*, 965 F. Supp. 731, 740 (D. Md. 1997) (granting summary judgment on question of whether actor had "exceed[ed] the authorization embodied in the confidentiality statements”). In the context of the CFAA, the Ninth Circuit has concluded that the phrase refers to those occasions when an actor is authorized to access certain data on a computer (like product information), but instead accesses different data on the computer (like customer data) for which the actor lacks authorization. *See United States v. Nosal*, 676 F.3d 854, 857–58 (9th Cir. 2012) (interpreting “exceeds authorized access” in the Computer Fraud and Abuse Act (CFAA)).

Given this statutory background, the relevant issue in this case is whether the location framework’s access of the phone’s RAM-stored location data violated the SCA. (Dkt. No. 69 at 23 (“Microsoft’s act of *searching* RAM for recent location information constitutes unauthorized access.”)); (Dkt. No. 97 at 5–6 (“[T]he SCA specifically prohibits unconsented *access* to data temporarily stored in RAM, regardless of tracking, and Microsoft does not dispute that it *accessed* each Class member’s RAM-stored location data without consent each and every time the Camera application was launched.”).) Even though Plaintiff frequently invokes the specter of Microsoft tracking users and crowd-sourcing location data (Dkt. No. 105 at 28), the subsequent uses (or misuses) of any data are not relevant considerations under this provision, which is concerned solely with unauthorized access. *See* 18 U.S.C. § 2701(a).

F. Access of RAM-stored location data

The Court first considers whether it was a violation of the SCA for the location framework on Plaintiff’s phone to access the RAM-stored location data each time the camera application launched. There is no dispute that Plaintiff left her phone’s master location switch on and at no time turned it off. By leaving that switch on, she allowed applications to call the location framework and thereby access her RAM-stored location data. (Dkt. No. 100 at 9–10.) The Court concludes that because Plaintiff granted this permission for Microsoft to access her location information, there was no unauthorized access when the location framework accessed that same information at the request of the camera application.[4] Because of this conclusion, the Court does not reach Microsoft's other arguments on summary judgment, including how to define the terms "facility" and "electronic storage" in the SCA. (Dkt. No. 100 at 18–25.)

Plaintiff argues that location data accessed at any particular moment is unique, (Dkt. No. 105 at 27 ("Location Framework worked . . . by . . . accessing *unique* location information that was *then-and-there* available and visible to the device.")), meaning that Microsoft lacked authority to access the unique location data available at the time the camera application opened. The Court is unconvinced for two reasons. First, Plaintiff does not demonstrate that the camera application was accessing unique data that no other application had access to. (Dkt. No. 105 at 27–28.) Second, even if Plaintiff did demonstrate this, the camera application's user prompt did not establish the sorts of nuanced authorization limits that would make such access unauthorized.

1. No evidence suggests that the information that was accessed when the camera application opened was different from the information that was accessed when other applications made requests.

There are two types of information that, for purposes of summary judgment, were apparently stored in RAM and therefore accessed: "*both* tiled Beacon data stored in RAM *and* Beacons "seen" by the device."[5] (Dkt. No. 27 n.17.) Regarding the first type of data, Defendant argues that there is "no evidence that the Camera app accessed location tiles [Plaintiff] had not previously authorized other [applications] to access." (Dkt. No. 100 at 17.) The Court agrees. The location framework accessed the same location tiles regardless of which application called it, and there is no dispute that Plaintiff authorized other applications to access the location tiles. (Dkt. No. 105 at 11.) Unlike a situation where different sorts of information were accessed, *see,*

[4] The Court uses "Microsoft" for ease of writing, but makes no determination about the parties' arguments concerning whether Microsoft (as opposed to a software component) can be judged to have accessed the location information. (Dkt. No. 100 at 7–8; Dkt. No. 105 at 22–23.)

[5] Plaintiff argues that there is no evidence that the "seen" Beacon data was not stored in RAM, so it is an issue of fact. (Dkt. No. 23 n.13.) The Court assumes for purposes of this order that this data is part of the accessed RAM-stored location data.

e.g., *Nosal*, 676 F.3d at 856, 858 (using as an example that an employee would "exceed[] authorized access" if he was permitted to access product information but instead looked at customer lists) the "unauthorized" access was of the same location tiles that Microsoft was authorized to access for different purposes. From this perspective, the location framework's use of the tiles to respond to a request from camera application was not an unauthorized access, but instead an unauthorized use. *See Educational Testing Serv.*, 965 F. Supp. at 740.

Plaintiff's argument in reply is somewhat unclear: "From the user's perspective, 'tiled' Beacon data *only* carries significance when associated with a temporal element—i.e., *when* Beacons were 'seen' by the phone, and *which* specific Beacons were in fact 'seen'—rather, it accessed her *then*-stored Beacon communications in an effort to determine where she was at that point in time." (Dkt. No. 105 at 28.) The Court understands Plaintiff's point to be that the available tiles were associated with a time stamp at some point.[6] To the extent that Plaintiff complains the tiles are associated with a time stamp and sent back to Microsoft, she is arguing about how the tiles are used once the location framework accesses them. And if Plaintiff's complaint is that the tiles were used to determine where she was at a given time even though she did not want such a determination made, that is also an unauthorized-use argument. Ultimately, Plaintiff does not contest Defendant's point that the same tiles might have been accessed by other applications. Instead, Plaintiff is complaining about the use of tiles (and their association with other data) to which Microsoft had authorized access.

Plaintiff also suggests that a second type of data—the Beacons "seen" by the device—were accessed without authorization. Even assuming that this data is appropriately considered to

[6] Plaintiff's citation in support is a document describing the packets of information sent back to Microsoft. (Dkt. No. 64-2 at 3 (describing the unique timestamp that accompanied "tracking information" in two example packets that were sent to Microsoft even if a user hit "cancel").) Although not a dispositive consideration, the Court notes that Plaintiff's citation discusses the packets sent back to Microsoft, and there is no evidence that those packets contained the same information as the tiles stored in RAM.

be RAM-stored location information, Plaintiff herself notes that the WM7 Background Scanners recurrently scanned Beacons to obtain "seen" Beacon data. (Dkt. No. 23 at 13; Dkt. No. 105 at 8 n.2, 23.) Plaintiff provides two record citations suggesting that this "seen" beacon information would have been unique when the camera application opened. The first is to the document that describes the background scanners. (Dkt. No. 106, ex. C.) The second is a developer design specification. (Dkt. No. 106, ex. D.) The Court has carefully considered these technical documents that were cited without supporting explanation or context, but neither appears to show that the beacons seen when the camera application opened would have been different than those seen when a different application opened. Indeed, if the report was not out of date, it appears that no scan would happen. Moreover, there is no suggestion that Plaintiff had or expected she had any control over the times at which the Background Scanner might scan for beacons, particularly in light of the fact that her master location switch was permanently on. In the absence of any such control, there is no evidence that information about "seen" beacons was accessed without authorization.

The Court concludes that there is no indication that Microsoft was "not entitled to see" the RAM-stored location data to which Plaintiff had granted it access by leaving her master location switch on. *Educational Testing Serv.*, 965 F. Supp. at 740. Summary judgment is therefore appropriate.

2. The camera application's user prompt did not impose authorization limits

Even assuming that Plaintiff is correct that unique location data was accessed when the camera application opened, a user prompt about whether the camera "can use your location" does not imply or impose nuanced authorization limits on when the location framework can access the phone's RAM. Plaintiff contends that her authorization limits were "express and specific," (Dkt. No. 105 at 22), and that "[she] *denied* Microsoft access to her location information when and where she used Camera." (Dkt. No. 105 at 28.) But on all occasions when she used Camera, her master location switch remained on and other applications had permission to access location data. No setting gave her control over the precise times that her phone's location framework would access the RAM-stored data. It is thus inaccurate to say that she denied Microsoft access to location information at any particular point in place or time. At most, she could simply have expected that her location information would not be used by the camera application. (Dkt. No. 105 at 10 (citing her "privacy expectation").) That is an expectation about the use of her data, not the access of her phone's RAM by a software component on her phone.

The Court is sympathetic to Plaintiff's claims that Microsoft's practices may have deceptive, but sympathy does not suffice when the statute creates liability only for unauthorized access. And although Plaintiff attempts to distinguish cases discussing the scope of authorized access (Dkt. No. 105 at 26–27), Plaintiff herself cites only one case, and that is merely a generic citation about her "reasonable expectation of privacy." (Dkt. No. 105 at 25.) Plaintiff is unable to conjure even one case in which the statute has been applied in a similar situation.

G. "Facility" under the SCA

Even if such access could create liability under the SCA, the Court also concludes that the mobile device as used here is not a "facility through which an electronic communications services ["ECS"] is provided." 18 U.S.C. § 2701(a). The SCA does not define "facility," but "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). And "electronic communications" are "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce [with four irrelevant exceptions]." 18 U.S.C. § 2510(12).

Here, the question is whether Plaintiff's phone provided an ECS and is a "facility" for purposes of the SCA. The court in *In re iPhone Application Litig.*, 844 F.Supp.2d 1040 (N.D. Cal. 2001) considered a nearly identical question. In that case, the plaintiffs alleged:

> Apple began intentionally collecting Plaintiffs' precise geographic location and

> storing that information on the iDevice in order to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States. . . . Apple represented that users could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iDevices to 'off.' Plaintiffs contend that Apple continued to monitor and store information about Plaintiffs' locations even when the functionality was disabled on users' iDevices.

In re iPhone, 844 F.Supp.2d at 1050. In considering this claim, the court recognized that some courts had issued non-binding decisions accepting that personal computers could be facilities but noted that those decisions had provided little analysis. *See id.* at 1057–58 (citing cases, including one from this court). "By contrast," the court wrote, "the courts that have taken a closer analytical look have consistently concluded that an individual's personal computer does not provide an electronic communication service simply by virtue of enabling use of electronic communication services." *Id.* (internal punctuation omitted) (citing *Crowley v. CyberSource Corp.*, 166 F.Supp.2d 1263, 1270–71 (N.D. Cal. 2001)).

The Court agrees with the *iPhone* court and the numerous cases following it. *See, e.g.*, *Roadlink Workforce Solutions L.L.C. v. Malpass*, No. 13-5459-RBL, 2013 WL 5274812, at *3 (W.D. Wash. Sep. 18, 2013) (following reasoning in *iPhone*); *Morgan v. Preston*, No. 13-0403, 2013 WL 5963563, at *5 (M.D. Tenn. Nov. 7, 2013) (citing numerous cases to demonstrate that "overwhelming body of law" supports conclusion that personal computer is not a facility); *Lazette v. Kulmatycki*, 949 F.Supp.2d 748, 755–56 (N.D. Ohio June 5, 2013) (explaining why reasoning in *iPhone* is persuasive). The Windows Phone 7 device is not a "facility through which an electronic service is provided" because the device enabled the use of the location services rather than providing them. *See Garcia v. City of Laredo*, 702 F.3d 788, 792–93 (5th Cir. 2012), *cert. denied*, 133 S. Ct. 2859 (2013) (discussing how cases, academic commentary, and legislative history support the conclusion that the relevant "facilities" are those operated by providers); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 11-1073, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012) ("[T]he relevant 'facilities' that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage.”). In this situation, Plaintiff's phone did not provide location services to other users in a server-like fashion, but instead received the relevant services from Microsoft. *See In re Pharmatrak Privacy Litig.*, 220 F.Supp.2d 4, 13 (D. Mass. 2002), *rev'd on other grounds*, 329 F.3d 9 (1st Cir. 2003) (personal computer must perform “server-like functions” in order to become “facility through which an electronic communications service is provided”). The fact that the phone not only received but also sent data does not change this result, because nearly all mobile phones transmit data to service providers. Moreover, reaching a contrary conclusion would, as Plaintiff seems to recognize (Dkt. No. 105 at 14 n.8), lead to the anomalous result that Microsoft could grant third parties access to Plaintiff's cell phone. *See* 18 U.S.C. § 2701(c) (entity providing electronic communications service can authorize access to a facility); *Crowley*, 166 F.Supp.2d at 1271 (recognizing this result and noting that it would ignore statutory language treating users and providers as different).

III. CONCLUSION

Given the Court’s ruling on Defendant’s summary-judgment motion, the Court finds the class-certification moot and does not address its merits. Defendant’s motion for summary judgment (Dkt. No. 100) is GRANTED, and Plaintiff's motion for class certification (Dkt. No. 70) is DISMISSED as moot.

DATED this 25th day of March 2014.

John C Coughenour

John C. Coughenour
UNITED STATES DISTRICT JUDGE